Memorable And Secure: How Do You Choose Your PIN?

A. Gutmann[1], M. Volkamer [1,2] and K. Renaud[3]

[1]Technische Universität Darmstadt, Germany
[2]Karlstad University, Germany
[3]University of Glasgow, United Kingdom
[1]firstname.surname@secuso.org
[3]firstname.surname@glasgow.ac.uk

Abstract

Managing all your PINs is difficult. Banks acknowledge this by allowing and facilitating PIN changes. However, choosing secure PINs is a difficult task for humans as they are incapable of consciously generating randomness. This leads to certain PINs being chosen more frequently than others, which in turn increases the danger of someone else guessing correctly. We investigate different methods of supporting PIN changes and report on an evaluation of these methods in a study with 152 participants. Our contribution is twofold: We introduce an alternative to system-generated random PINs, which considers people's preferred memorisation strategy, and, secondly, we provide indication that presenting guidance on how to avoid insecure PINs does indeed nudge people towards more secure PIN choices when they are in the process of changing their PINs.

Keywords

Authentication, PINs, PIN change, user advice

1. Introduction

Computer systems need to confirm the identity of their users, and the most widely used mechanisms are knowledge-based PINs and passwords. Both are essentially secrets that should not be divulged to others. People are expected to keep multiple such secrets in their memory, memorising a new entry each time a new PIN or password is added. The problem is that human memory is fallible and this can result in loss of secrets or interference between memorised secrets.

PINs are banks' preferred knowledge-based authentication and are thus a fact of life. Therefore it is worth considering how we can support customers in managing their PINs. While PINs appear in other contexts too, we decided to focus our research on banking-related scenarios. Our intention thereby is to encourage security-oriented decisions while acknowledging the need for memorisation. In this context, previous work has focused on determining people's mental model of PIN management (Renaud and Volkamer, 2015) and on deriving guidance to assist people in memorising their PINs (Gutmann *et al.*, 2015). However, people might alternatively want to ease their memory load by exercising their ability to change and/or record their PINs. Many banks forbid PIN recording, despite many bank customers

admitting to engaging in this practice anyway. But banks do acknowledge the difficulties people experience in retaining all their PINs by allowing and facilitating PIN changes (Murdoch *et al.*, 2016). Thus the pragmatic course of action is to iterate on the benefits of changing PINs and to direct people towards stronger decisions as and when they are about to change their PIN. The obvious question left is: "What kind of assistance we can provide to bank customers when changing their PINs?"

In general, there are two means to change PINs: (1) Manually choose one at an ATM, or (2) request the bank to generate and issue a new random PIN. A notable drawback of the second option is that banks usually issue new PINs by mail, which involves a significant time delay. The problem with self-chosen PINs is that humans are generally incapable of consciously generating randomness (Figurska *et al.*, 2008) and there is further evidence to show that many people do indeed choose insecure PINs (Bonneau *et al.*, 2012) (DataGenetics, 2012). In this paper we investigate people's preferred methods to change PINs through a study with 152 participants. Our main contributions are:

1. We suggest an alternative method of generating random PINs: ask the user for their preferred memorisation strategy and issue a PIN that matches their preferences.

2. We report on indications that people who opt to receive PIN-changing advice seem to indeed choose more secure PINs.

We introduce and motivate the integral parts of the PIN change procedure Section 2. Section 3 examines this procedure with a PIN change survey. The result of this survey is presented in Section 4 and discussed in Section 5. In Section 6 we discuss related work. In Section 7 we draw conclusions and describe future work. Finally, Section 8 states the limitations of this paper.

2. PIN change procedure

In previous research a study was carried out to explore people's mental models with respect to PIN management (Renaud and Volkamer, 2015). With respect to PIN changing, therein was reported that people changed their PINs to improve memorability, when their bank required it, and when they had lent their bank card to someone else. These reasons offer fruitful avenues for providing support depending on the card holder's needs by encouraging and supporting more secure choices. But as the reasons for changing differ, so should the provided assistance be flexible. Thus a PIN change procedure should provide multiple options catering to people's needs.

We designed and tested a PIN change procedure that provides a user with different options and empowers them by allowing them to choose the most suitable strategy. Our suggestion is composed of four options: (a) Generate a new PIN for those who feel confident memorising the next number, but question their ability to choose a secure one. (b) Generate a new PIN tailored to some specified memorisation strategy for those who have difficulty choosing a secure PIN which they can memorise easily.

(c) Provide an option to allow the user to choose a PIN for those who have difficulty memorising numbers and are confident that they know how to choose a secure PIN. (d) Provide recommendations for choosing a PIN to those who have difficulty memorising numbers and are open to advice on how to choose secure PINs.

For option (b), we further decided to provide three memorisation strategies in this study: (1) Visualisation: visualising the shape the PIN makes when being entered, (2) Arithmetic: splitting the PIN up into two two-digit numbers and memorising these or performing some arithmetic on the two halves, and (3) Dictionary: memorising a word from the letters imprinted on the PIN's corresponding buttons on many PIN pads. Our third strategy is not among the three most popular memorisation strategies in previous work (which would have included Association: associating the PIN with some already known number) but was mentioned, too (Renaud and Volkamer, 2015). Our reason for this substitution is that we assume it to be unrealistic to emulate an association to a number already known to the participants unless we'd pick well-known numbers such as the year 1945, a practice that is ill-advised (Bonneau *et al.*, 2012) (DataGenetics, 2012).

Option (a) is supposed to primarily satisfy those who change their number after being ask to by their bank or after having lent their card to someone else, while option (b) to (d) are intended to cater to those who change their PIN to improve memorability.

3. PIN change survey

We conducted a survey to investigate user decisions and behaviours when confronted with our suggested PIN change procedure. Since anything related to banking and money can be expected to be a sensitive topic, we opted for an online study in order to provide our participants' an appropriate feeling of anonymity.

3.1.1. Attitude towards PIN change

In order to estimate the participants' general attitudes, our survey began with a question regarding their opinion of bank customers being permitted to change their PINs.

3.1.2. Scenario

Participants were confronted with the scenario of having received a 4-digit PIN and being worried about having difficulties remembering it. The scenario suggests that they would consider changing it. The participants were asked whether this constituted a realistic scenario for them. Those who confirmed proceeded to the PIN change options. Those who declined were presented with four intermediate questions: We asked them why the scenario was not realistic, how they usually memorised their PINs, how they would recommend others to memorise their PINs, and what they would recommend to others who wanted to change their PINs.

Thereafter an alternative scenario described a situation where they were to assume that someone had observed them entering their PIN and they wanted to change it.

3.1.3. PIN change options

Before being presented with the actual PIN change options, participants were asked whether they would either like their bank to issue them with a new PIN or whether they would like to change it themselves at an ATM.

Those who wanted their bank to change it were presented with options (a) and (b), as described in section 2. In short, these options provided were (a) a new random PIN and (b) a procedure were the participant was first presented with a list of memorisation strategies, asked to choose one, and then issued a new PIN matching the preferred memorisation strategy. A picture of an ATM PIN pad supplemented the presented memorisation strategies and explanations, which read: *Visualisation:* The movement of a finger entering the PIN results in a pattern, e.g. 2589 depicts the letter L. *Arithmetic:* A mathematical operation on one part of the PIN results in the other, e.g. 4812 can be memorised with 48 / 4 = 12. *Words:* Many PIN pads display letters that can be used to memorise a word, e.g. 5683 corresponds to the word LOVE.

Those who wanted to change their PIN via an ATM were given the same options as above, including the supplemented picture of an ATM PIN pad, plus PIN change options (c) and (d). These two options hadn't been available for those who asked their bank to change the PIN for them, as that would have been a contradiction to options (c) and (d) being about choosing the PIN themselves. In short, these options were: (c) choosing a new PIN themselves, or (d) being provided with a list of guidelines to help them choose a secure PIN. Those guidelines were derived by us based on a webpage on PIN analysis (DataGenetics, 2012) and stated: (1) Use three different numbers, but not four consecutive numbers. (2) Don't use your birthday or that of close friends or relatives.

No participant had the opportunity to change their mind after having already chosen a PIN change option. Those participants who chose option (a) or (b) hadn't seen the provided PIN beforehand to ensure their decision was based on the option itself. They further were told that it had been randomly generated, but it was actually the same number for all participants. We included that information in the debriefing at the end of the survey.

3.1.4. Questionnaire

After the previous step had ensured that the participants had completed the mental workload of choosing a new PIN, we asked them a series of questions to better understand their choices and to be able to better compare the PIN change options (a) to (d). Those questions were: (1) Why did you choose this option? (2.1) How would you rate the memorability of PINs generated with this option? (2.2) Please explain your rating. (3.1) How would you rate the security of PINs generated with this option? (3.2) Please explain your rating. (4) Did we miss out a viable PIN changing option?

3.1.5. Demographics

The survey ended with demographic questions regarding the participants age, number of PINs held (and number of unique PINs) across all devices, and a self-assessment on a five-scale rating to the following statements: (1) “I am experienced with PINs. ”, (2) “I have difficulties with PINs”, and (3) “I don’t need assistance with managing my PINs.”

3.1.6. Debriefing

Finally, the survey ended with participants being displayed a text for debriefing.

4. Results

We recruited 152 participants who reside in the United Kingdom via ClickWorker, an online crowd-sourcing platform. Our participants were aged between 18 and 64, and on average 33 years old and generally had a positive attitude towards being permitted to change their PINs at an ATM. 146 participants (96%) were positive, stating diverse reasons such as security, memorability, and being in control. Two participants had no opinion and 4 expressed security concerns.

The majority of all participants (90.1%) rated the presented scenario as realistic. The remaining 15, two of whom disapproved of PIN changes, stated ease of memorisation as their reason for rejecting the scenario and one disclosed that he usually contacted his bank to ask for assistance in managing new PINs. Their recommendations for PIN management were either (1) using memorisation strategies, (2) writing it down in a secure and offline manner, or (3) to contact their bank and ask for assistance.

Over two thirds of all participants (67.8%) preferred to change the PIN at an ATM, rather than ask their bank for a new one. This proportion increased to 73% in the group that acknowledged PIN memorising difficulties.

Of those 49 who stated that they would ask their bank for a new PIN, 25 preferred a randomly generated PIN—(option (a)—and 24 the option based on memorisation strategies—option (b). Considering only those with potential memorability issues, the numbers change to 11 and 23, respectively.

Of those 103 participants who chose to change their PIN via an ATM, only three considered the memorability scenario as unrealistic. The majority (77%) preferred to choose a new PIN without assistance—option (c)—and 18 participants (17%) opted for the guidelines—option (d). A further three chose to receive from options (a) and (b), each.

Among all participants who chose option (b)—27 participants in total—the visualisation and dictionary strategies (41% and 44% respectively) were the preferred methods.

On being asked why they chose the respective PIN change option, over two thirds (72.4%) of participants cited ease of memorisation. 24 participants made their choice to maximise perceived security and six named convenience as their main motivation. One participant mentioned 'being in control' and another mistrusted the integrity of ATMs as their sole motivation. Ten participants considered this kind of information too sensitive to divulge in an online survey.

The rating on the memorability and security of all four PIN change methods is depicted in Figures 2 and 3. 138 participants justified their rating of the memorability with the perceived ease of memorisation, 7 with the number having no meaning and 7 with their intuition. More than every second participant (55.3%) based their rating of the security on how difficult they assume it would be to guess the PIN. 22.4% each stated their intuitive feeling or their exclusive knowledge of the PIN as reason. Few people further expressed mistrust towards the integrity of their bank's procedure when issuing new PINs. They assume decreased security of PINs issued this way and therefore consider changing every banking PIN at an ATM as only viable option. While no one reported any missing PIN change options, two alternatives were mentioned: (1) changing a PIN via online banking and (2) on the telephone.

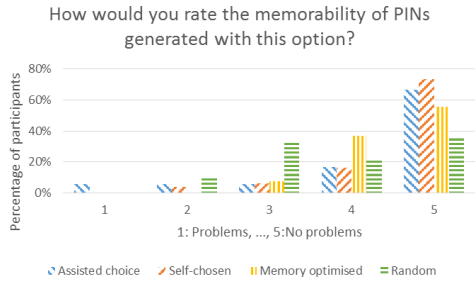

Figure 1: Ratings on the memorability of the provided PIN change options.

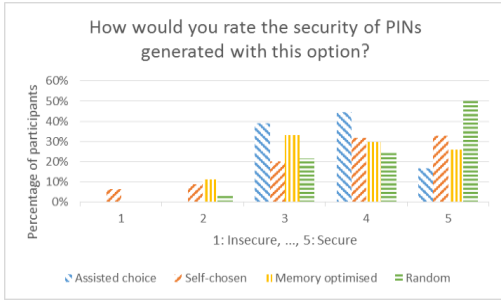

Figure 3: Ratings on the security of the provided PIN change options.

The general tendency on the self-report statements was that people judged themselves as being experienced with PINs, experiencing relatively few difficulties and seldom requiring assistance. The detailed results are presented in Table 1 and participant demographics are reported in Table 2.

Agreement to statements (1: agree, …, 5: disagree)	**1**	**2**	**3**	**4**	**5**
"I am experienced with PINs."	65%	21%	11%	3%	1%
"I have difficulties with my PINs."	2%	11%	7%	28%	53%
"I don't need assistance managing my PINs."	52%	18%	6%	10%	13%

Table 1: Participant's experience with PINs as self-reported.

Demographics	**Average**	**Median**	**Maximum**	**Minimum**
Age	33	30	62	18
Number of PINs	5.2	3	15	1
Number of unique PINs	4.4	2	15	1

Table 2: Demographic data as self-reported by participants.

Lastly some participants volunteered interesting pertinent remarks: (1) "A PIN reminder service (not PIN change) can be a lifesaver - banks must provide this at all hours, particularly if customers are not allowed to choose their own PIN." (2) "There are many possibilities of ways to change PINs which just haven't been put into use yet. Electronic devices, online, mobile." (3) "There should be more swipe option cards available now but security needs to be improved."

5. Discussion

We set out to explore the best form of advice we could formulate in order to guide bank customers towards better PIN choice. The first finding of note was that 90% of participants considered it realistic to have difficult memorising a newly issued PIN. At first glance, this might be in contrast to most people not requiring assistance with their PINs (see statement "I don't need assistance managing my PINs." in Table 1). On second thoughts it makes sense if they had already developed a coping strategy for such situations. This explanation is further supported by two third of participants choosing to change their PINs at an ATM instead of requesting a new PIN from their bank. Furthermore, this does confirm previous findings with respect to people rejecting efforts to advise them if they don't feel that they need such advice (Renaud and Volkamer, 2015). The open text responses also seem to confirm this.

Of those who wanted to change the PIN themselves at an ATM, 77% didn't want recommendations on choosing a new PIN. It might be that the ATM affords a measure of *autonomy* in their choices. On the other hand it could be that self-driven changing was the most familiar option. Since people favour *familiarity* (Maslow, 1943) this could have played a role. Neal *et al.* (Neal *et al.*, 2006) explain that habits, once entrenched, constitute part of the person's self-concept. Hence, expecting people to change the way they do things, simply because they are given some advice, is clearly unrealistic.

When analysing PINs of a small sample, it is difficult to draw reliable inferences. We thus compared the chosen PINs with statistics reported by DataGenetics (DataGenetics, 2012). Three out of eighteen participants (17%) who saw the guidelines chose common, weak PINs: 1971 ("memorable year"), 1213 ("easy to remember") and 1963 ("year of birth, but not birthday"). 24 out of 79 (30%) who declined guidelines chose common PINs: 1234 (8 times), 0000 (4 times), 1111 (3 times), 1990, 5678, 1968, 2266, 1511, 3232, 9876, 1212, and 2662. All would have been discouraged by our guidelines (1990 and 1968 are, as was stated in the comments, the participant's years of birth). This indicates that people who opt to receive advice while changing their PIN do make more secure decisions.

6. Related work

Banks, who issue PINs, commonly offer advice to their customers such as to *personalise* their PIN when changing it (Murdoch *et al.*, 2016), something that is open to a wide range of interpretation. As the DataGenetics webpage (DataGenetics, 2012) shows, this changing is likely to have led to more than 10% of PINs being 1234, which hardly seems personal but is undeniably memorable.

Some researchers have attempted to help people retain their PINs. For example, Renaud and Smith (Renaud and Smith, 2001) proposed a mechanism called "Jiminy" to support secure recording of PINs, but users found it too laborious. Jiminy is a software tool that creates a grid of numbers, which could be publicly displayed, superimposed onto an image. A coloured template, which was securely stored, revealed the PIN. The Spydeberg Sparebank came up with an alternative mechanism which assists customers by providing a credit-card sized cut-out. The customer is instructed to write the PIN in the grid, using a particular combination of colours and positions. This scheme was shown to be insecure, since people demonstrate predictability by often using the top left-hand corner of such a grid as an anchor (Andriotis *et al.*, 2014).

Some researchers have attempted to help people by providing them with easy memorisation techniques. A promising mechanism that could be used for PINs is mnemonics, where you try to make a sentence from the PIN (Bellezza, 1992). So, if the PIN were 3822 you might say three men and 8 dogs caught 22 rats. The power of mnemonics is even observed in older adults who often find memorisation challenging (Derwinger *et al.*, 2003). Jakobsson and Liu propose deliberately generating PINs that create a meaningful mnemonic when typed in (Jakobsson and Liu, 2011). They carried out a usability study with 25 participants and three failed initially to understand how to enter their PIN, which might be too high for banks to accept. Recent attempts on providing guidance to better PIN management were based on PIN related mental models (Renaud and Volkamer, 2015), (Gutmann *et al.*, 2015). Marky *et al.* mentioned an implementation thereof as a privacy preserving application for mobile phones (Marky *et al.*, 2016).

When providing guidance and advice, people's very basic and profound need for *autonomy*, *competence* and *relatedness* has to be considered (Reis, 2000). With

respect to *autonomy*, Ryan (Ryan, 1993) explains that people engage in a reflective evaluation of their options which involves consideration of the person's interests and needs. Hence advice has to appeal to a person's self-interest and needs. With respect to *competence*, by taking advice a person implicitly acknowledges that they are less than competent in a particular area. Gino and Moore (Gino and Moore, 2007) found that people were more willing to accept advice if the task was considered to be difficult. Choosing a PIN is hardly difficult *per se* so people might be unwilling to acknowledge any lack of competence in this respect. Considering *relatedness*, Harvey *et al.* (Harvey *et al.*, 2000) explain that people will take advice if they consider the advice giver to be more experienced than they are. It seems that a new PIN holder might be willing to accept advice, but that others, having worked out PIN strategies for themselves in the past, might be less open to advice.

7. Conclusion and future work

Our motivation for this research was that we saw the need for people to be given some guidance when they choose a new PIN. This, we felt, would make PINs less predictable, and thus more resilient to compromise. We discovered indicators that presenting people with guidelines on how to choose a secure PIN does improve security. Even though our sample was too small to infer a definite improvement, we recommend banks to implement such guidance! Future work should investigate confirming or rejecting our observation and on how such advice should best be designed to maximise its efficacy.

Regarding the generation of random PINs we introduced a method that is promising on improving the memorability without significantly reducing the security. But our study didn't thoroughly evaluate this method and most insights remain hypotheses. We see promising indicators and believe that this method has potential, but we also cautiously recommend further investigation before considering an implementation.

8. Limitations

Questioning people about PIN-related behaviour is a sensitive task. We conducted an online survey in order to guarantee anonymity. Such a procedure is always reliant on self-report and might sometimes have been performed under time pressure or distraction. 10 participants were unwilling to talk about their motivation for choosing a particular PIN change option. It might have been something they considered too sensitive to disclose. We cannot guarantee that their other responses were truthful either, but we were reluctant to exclude them since that might falsify our results. We hope that they simply declined to answer questions rather than giving false information in responses. Fabrication is a limitation of any study, even those carried out in a lab. We acknowledge this but do not know how to ameliorate it.

9. References

Andriotis, P., Tryfonas, T. and Oikonomou, G. (2014). "Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method". Human Aspects of Information Security, Privacy, and Trust, pp. 115-126.

Bellezza, F.S., Six, L.S. and Phillips, D.S. (1992). "A mnemonic for remembering long strings of digits". Bulletin of the Psychonomic Society, Vol. 30, No. 4, pp. 271-274.

Bonneau, J., Preibusch, S. and Anderson, R. (2012). "A birthday present every eleven wallets? The security of customer-chosen banking PINs". Financial Cryptography and Data Security, pp. 25-40.

Derwinger, A., Neely, A.S., Persson, M., Hill, R.D. and Bäckman, L. (2003). "Remembering numbers in old age: Mnemonic training versus self-generated strategy training". Aging, Neuropsychology, and Cognition, Vol. 10 No. 3, pp. 202-214.

Figurska, M., Stańczyk, M. and Kulesza, K. (2008). "Humans cannot consciously generate random numbers sequences: Polemic study". Medical hypotheses, Vol. 70, No. 1, pp. 182-185.

Gino, F. and Moore, D.A. (2007). "Effects of task difficulty on use of advice". Journal of Behavioral Decision Making, Vol. 20, No. 1, pp. 21-35.

Gutmann, A., Renaud, K., and Volkamer M., 2015. "Nudging Bank Account Holders Towards More Secure PIN Management". Journal of Informatics and Secure Transactions, Vol. 4, No. 2, pp. 380-386.

Harvey, N., Harries, C. and Fischer, I. (2000). "Using advice and assessing its quality". Organizational behavior and human decision processes, Vol. 81, No. 2, pp. 252-273.

Jakobsson, M. and Liu, D. (2011). "Bootstrapping mobile PINs using passwords".

Marky, K., Gutmann, A., Rack P., and Volkamer M. (2016). "Privacy Friendly Apps-Making Developers Aware of Privacy Violations". 1st International Workshop on Innovations in Mobile Privacy and Security, pp. 46-48.

Maslow, A.H. (1943). "A theory of human motivation". Psychological review, Vol. 50, No. 4, p.370.

Murdoch, S.J., Becker, I., Abu-Salma, R., Anderson, R., Bohm, N., Hutchings, A., Sasse, M., and Stringhini, G.(2016). "Are Payment Card Contracts Unfair?" Financial Cryptography.

Neal, D.T., Wood, W. and Quinn, J.M. (2006). "Habits—A repeat performance". Current Directions in Psychological Science, Vol. 15, No. 4, pp.198-202.

PIN number analysis (2012). "PIN number analysis", www.datagenetics.com/blog/september32012/index.html, (Accessed 18 March 2016).

Reis, H.T., Sheldon, K.M., Gable, S.L., Roscoe, J. and Ryan, R.M. (2000). "Daily well-being: The role of autonomy, competence, and relatedness". Personality and social psychology bulletin, Vol. 26, No. 4, pp. 419-435.

Renaud, K. and Smith, E. (2001). "Jiminy: helping users to remember their passwords". Annual Conference of the South African Institute of Computer Scientists and Information Technologists, pp. 73-80.

Renaud, K. and Volkamer, M. (2015). "Exploring Mental Models Underlying PIN Management Strategies". World Congress on Internet Security, pp. 18-23.

Ryan, R.M. (1993). "Agency and organization: Intrinsic motivation, autonomy, and the self in psychological development".